UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA :

- v. - :

MATHEW MARTOMA, :

Defendant. :

S1 12 Cr. 973 (PGG)

GOVERNMENT'S MOTION *IN LIMINE* TO ADMIT EVIDENCE CONCERNING THE DEFENDANT'S EXPULSION FROM HARVARD LAW SCHOOL IN RESPONSE TO POTENTIAL DEFENSES

PREET BHARARA
United States Attorney for the
Southern District of New York
Attorney for the United States
of America.

Arlo Devlin-Brown
Eugene Ingoglia
Assistant United States Attorneys

PRELIMINARY STATEMENT

The Government hereby moves *in limine* to offer pursuant to Federal Rule of Evidence 404(b) certain evidence relating to the expulsion of Mathew Martoma (the "defendant") from Harvard Law School (the "Harvard Evidence") in the event that the defense offers evidence or arguments that make the circumstances surrounding the expulsion relevant to disputed issues at trial.[1] In particular, the Government understands that the defense may involve claims that (i) the Government's inability to find computer forensic evidence establishing Martoma possessed a key document containing inside information and/or (ii) evidence or argument purporting to show that computer forensic evidence supports an inculpatory version of events. The Harvard Evidence demonstrates both Martoma's knowledge of the importance of minimizing the existence of incriminating electronic traces and of his ability to create sophisticated forgeries and alterations of such evidence. In particular, the Harvard Evidence establishes, in substantial part through uncontested and readily established facts, that the defendant: (i) used computer software to generate a forged Harvard Law School transcript, which was submitted to federal judges in connection with Martoma's clerkship applications; (ii) fabricated phony e-mail evidence which Martoma then submitted to the Harvard Law School Administrative Board (the "Ad Board") to bolster a false defense; and (iii) in an effort to appeal the Ad Board's decision to expel him, submitted to Harvard Law School a phony report from a supposed computer forensics firm the defendant had in fact created himself purporting to provide additional forensic evidence supporting Martoma's claims. Accordingly, the Government would seek to offer the Harvard Evidence under Rule 404(b) as evidence of the defendant's capacity to destroy or fabricate

[1] At the defendant's request, the Government has not yet publicly filed this motion in order to afford the Court an opportunity what the Government understands will be a defense request to maintain this motion and related proceedings under seal. This does not reflect any view by the Government that the motion should be sealed, however.

electronic forensic evidence in the event certain defenses about the forensic evidence or lack thereof make these issues relevant.

RELEVANT FACTS

The PowerPoint Presentation

Superseding indictment 12 Cr. 973 ("the Martoma Indictment") charges Martoma with obtaining from Dr. Gilman an advance preview of highly confidential drug trial results that Dr. Gilman would publicly present at a medical conference (the "ICAD conference") on July 29, 2008. In particular, as charged in the Indictment, Dr. Gilman was "unblinded" to the drug trial results on July 15, 2008 and July 16, 2008 by Elan and Wyeth personnel in San Francisco. After returning home to Ann Arbor, Michigan, Dr. Gilman received by e-mail on the afternoon of July 17, 2008 a draft of a PowerPoint presentation of the drug trial results that Dr. Gilman was to deliver at ICAD. The Indictment alleges that Dr. Gilman then described the PowerPoint slides in a phone call with the defendant later that afternoon and that Martoma then flew from New York to Detroit and back on Saturday, July 19 to meet personally with Dr. Gilman in his Ann Arbor office. Dr. Gilman will testify that, in addition to the above, he recalls sending the PowerPoint presentation to Martoma via e-mail. There is no computer forensic evidence, however, establishing that Martoma had an electronic copy of the PowerPoint presentation before the public announcement, whether obtained via e-mail or other means.

Potential Defenses Relating To The PowerPoint Presentation

Martoma has not identified a defense to the allegations discussed above, but various defense correspondence and motions have suggested that the defendant attaches significance to the lack of forensic proof that the he possessed the incriminating PowerPoint presentation before it was public. One potential line of defense might therefore be that the Government's inability to

find an electronic copy of the PowerPoint presentation on Martoma's SAC Capital e-mail account or in his electronic files tends to prove that Martoma never had early access to the drug trial results at all. A second potential line of defense – more speculative, but one that the defendant declines to rule out – would be to argue that other computer forensic evidence (including, potentially, new evidence to be offered by the defense) provides affirmative proof that the defendant did not receive an electronic copy of the PowerPoint presentation, or received it only after the presentation had been made public.

The Harvard Evidence

The Government proffers that it could establish the following evidence – in substantial part based on the defendant's admissions before the Ad Board and other evidence he adopted as accurate in that proceeding – relating to Martoma's expulsion from Harvard Law School. Most of this evidence is reflected in a seven page document issued by the Ad Board reporting its findings, attached hereto as Exhibit A.[2]

According to undisputed evidence presented to the Ad Board, Martoma used computer software in December 1998 to create forged Harvard Law School transcript, one that altered the first year grades reported on his official transcript by changing several B grades to As. Ex A. ¶ 1. In late December 1998 or early January 1999, Martoma's forged transcript was sent to 23 judges in connection with clerkship applications submitted to 23 judges in the United States Courts of Appeals. *Id.* at ¶ 2. On January 26 and January 27 Martoma interviewed for clerkship positions with three judges on the D.C. Circuit Court of Appeals, knowing that they had received the transcript Martoma had forged and failing to disclose this fact. *Id.* at ¶ 3 and ¶ 4. On February 2, Martoma was summoned to the Harvard Law School registrar, who informed

[2] During the relevant time frame Martoma used the name Ajay Mathew Thomas. Following his expulsion, he changed his legal name to Mathew Martoma. For convenience, this memorandum will consistently use "Martoma" rather than alternating between the names.

Martoma that his altered transcript had been detected. *Id.* at ¶ 8. Martoma admitted he had altered the transcript told the registrar "it was all a joke." *Id.* at ¶ 9. After speaking with the Registrar, Martoma met with Harvard Law School's Dean of Students, acknowledging again that he had forged his transcript and claiming that "the application was a joke and that [he] really did not intend to pursue a clerkship." *Id.* at 9. Martoma also told the Dean of Students that he "had already sent withdrawal letters to the judges." *Id.*

In the Ad Board proceedings, Martoma abandoned his initial defense that sending forged transcripts to federal judges to obtain a clerkship had merely been a "joke," claiming instead that he had forged the transcript only to show it to his parents (before changing his mind and showing them the real one a few days later) and that it ended up being received by judges only because Martoma had relied on his family to photocopy and assemble the various parts of the clerkship applications and that Martoma's brother had, despite Martoma's instructions about where to find the real transcript, stumbled upon the fake transcript and copied that one accidentally. *Id.* at 3. Martoma did stand by his claim that he had "already sent withdrawal letters" before Harvard had confronted him with the forgery on the afternoon of February 2, offering as support a withdrawal letter dated January 31, 1999, and an e-mail dated stamped February 1, 1999 informing the secretary for a Harvard Law School professor that Martoma was withdrawing his clerkship applications and no longer needed letters. *Id.* at ¶ 11 and 4.

The evidence Martoma submitted in the Ad Board proceeding involving his creation of a forged transcript was itself the product of forgery. Uncontested evidence established that the withdrawal letters to the judges that Martoma had dated "January 31, 1999" were in fact sent in envelopes postmarked February 3, 2009, a full day after Martoma had been confronted. *Id.* at ¶ 11. The e-mail, though, was the much more sophisticated forgery. Not only did the date read

"February 1, 1999" in the text of the e-mail, but the electronic metadata associated with the e-mail appeared to show it had in fact been created on February 1, 1999 as indicated. *See* Exhibit B, attached, at 1. But the e-mail and its metadata had been faked. Harvard Law School server records proved that Martoma's withdrawal e-mail dated February 1 e-mail was not transmitted until February 2 at 10:20 p.m., hours after Martoma had been confronted. *See* Exhibit A at ¶ 10. Worse, other e-mail metadata contained in the header information (Exhibit B at 2), showed that the e-mail Martoma claimed to have sent on February 1 was a reply to an e-mail that Martoma had not himself received until February 2. Exhibit A at 4; Exhibit B at 2.[3] Martoma could simply not have "replied" on February 1 to an e-mail he had not even then received. On May 12, 1999, the Ad Board voted to recommend Martoma's expulsion from Harvard to the faculty.

Incredibly, Martoma's response to the Ad Board's expulsion recommendation was to create still more false forensic evidence, the most elaborate yet, in an effort to reverse the decision through Harvard's administrative appeals process. In particular, Martoma and a business partner who was facing federal fraud charges created a bogus company called "Computer Data Forensics" to generate forensic evidence that would support Martoma's position. Martoma himself created a brochure for the company replete with false information about the company's extensive experience. Martoma then provided a "report" from Computer Data Forensics (signed by three temp agency employees with no training or experience in computer forensics, and who had not conducted any forensic examination) purporting to explain away the fraudulent February 1 e-mail Martoma had previously concocted based on new forensic evidence recovered from Martoma's laptop. (The report and brochure are attached hereto as

[3] Indeed, Martoma's attorneys informed the Harvard Ad Board that a computer forensic expert that the law firm had arranged to provide evidence in Martoma's defense had withdrawn upon learning that the supposed February 1 e-mail had been sent as a reply to an e-mail that Martoma had not received until the next day, reporting that "he was not in a position to authenticate" the defendant's version of events. *See* Exhibit A. at 5.

Exhibit B).[4] The report, loaded with impressive sounding techno-jargon (e.g., "[w]e used CRCMD to authenticate data at both a physical level and logical level") fooled the Harvard Law School professor handling Martoma's appeal, who issued a decision affirming Martoma's dismissal but describing the e-mail evidence as being a much closer question in light of the supposed forensic findings Martoma had fabricated.

APPLICABLE LAW

Federal Rule of Evidence 404(b), which addresses the admission of "other act" evidence and can serve as a separate basis for the admission of uncharged conduct provides, in relevant part:

> Evidence of other crimes, wrongs, or acts is not admissible to prove the character of a person in order to show action in conformity therewith. It may, however, be admissible for other purposes, such as proof of motive, opportunity, intent, preparation, plan, knowledge, identity, or absence of mistake or accident

It is well-settled that "other acts" evidence is admissible under Rule 404(b) as long as the evidence: (1) is advanced for a proper purpose; (2) is relevant to the crimes for which the defendant is on trial; and (3) has probative value that is not substantially outweighed by any unfair prejudicial effect. *See, e.g., United States* v. *Guang*, 511 F.3d 110, 121 (2d. Cir. 2007) (citations omitted) *See also States* v. *Brand*, 467 F.3d 179, 196 (2d Cir. 2006). The Second Circuit takes an "'inclusionary" approach to the admission of prior act evidence, under which "evidence of prior crimes, wrongs, or acts 'is admissible for any purpose other than to show a defendant's criminal propensity'" so long as it is not substantially outweighed by the danger of

[4] The Government could prove much of the evidence involving the Computer Data Forensics fraud through Martoma's own prior statements. In a statement given to the FBI in 2000 relating to the criminal activity of his business partner, Martoma – while blaming his partner for much of what happened at Computer Data Forensics – admitted establishing the company and drafting the brochure describing its supposedly legitimate services, and described the company's employees as untrained temp workers with no experience in computer forensics.

unfair prejudice. *United States* v. *Paulino*, 445 F.3d 211, 221 (quoting *United States* v. *Pitre*, 960 F.2d 1112, 1118-19 (2d Cir. 1992)); *see also United States* v. *Teague*, 93 F.3d 81, 84 (2d Cir. 1996) (providing that proof of state of mind, such as intent, is a "proper purpose" for admission of other crimes evidence under Rule 404(b) (quoting *Huddleston* v. *United States,* 485 U.S. at 691)); *see also United States* v. *Ortiz*, 857 F.2d 900, 903 (2d Cir. 1988) ("[O]ther acts or crimes are admissible under Rule 404(b) to prove matters other than the defendant's criminal propensity").

The Court has broad latitude in determining whether to admit evidence pursuant to Rule 404(b), and its ruling will be reviewed only for abuse of discretion. *See, e.g.*, *United States* v. *Guang*, 511 F.3d 110, 121 (2d. Cir. 2007); *United States* v. *Mitchell*, 328 F.3d 77, 82 (2d Cir. 2003). If requested, such evidence must be admitted with limiting instructions to the jury. *See United States* v. *Zackson*, 12 F.3d 1178, 1182 (2d Cir. 1993); *United States* v. *Ramirez*, 894 F.2d 565, 568 (2d Cir. 1990) (citing *Huddleston* v. *United States*, 485 U.S. 681, 691-92 (1988)).

Rule 404(b) expressly permits the admission of evidence of "knowledge" as well as "opportunity." Fed. R. Evid. 404(b). "To show 'opportunity' is to show that the defendant had some special capacity, ability or knowledge that would enable him to commit the crime." *United States* v. *Maravilla*, 907 F.2d 216, 222 (1st Cir. 1990) (Breyer, J.); *see also United States* v. *Murray*, 618 F.2d 892, 900 (2d Cir. 1980); *United States* v. *Green*, 648 F.2d 587, 592 (9th Cir. 1981) ("'Opportunity' is an express exception of Rule 404(b). Though the word has been little used by the courts it evidently is intended to cover all or a part of a category called 'capacity.'. . . The exceptions of knowledge, plan, motive, and opportunity are all closely related."); *cf. United States* v. *Zedner*, 401 F.3d 36, 49 (2d Cir. 2005), *rev'd on other grounds,* 126 S. Ct. 1976 (2006) (evidence of prior fraud admissible because it tended to prove "financial sophistication, his

ability to execute complex schemes, and his ability to form intent to defraud"). The ability to commit a crime includes the ability to do so in a manner that minimizes the risk of detection. *See United States v. Bailey*, 133 Fed. Appx. 534 at *3 (10th Cir. 2005) (evidence of prior drug dealing relevant to establishing defendant's ability distribute drugs in a manner that reduced risk of detection).

Other acts evidence is, like all other evidence, inadmissible under Rule 403 if its probative value is substantially outweighed by the danger of unfair prejudice. *See* Fed. R. Evid. 403. *See also United States* v. *Roldan-Zapata*, 916 F.2d 795, 804 (2d Cir. 1990); *United States* v. *Smith*, 727 F.2d 214, 220 (2d Cir. 1984). Evidence is unfairly prejudicial, however, "only when it tends to have some adverse effect upon a defendant beyond tending to prove the fact or issue that justified its admission into evidence." *United States* v. *Figueroa*, 618 F.2d 934, 943 (2d Cir. 1980).

ARGUMENT

As noted above, in determining whether to admit evidence pursuant to Rule 404(b), a court is must assess (1) whether the evidence is offered for a proper purpose and (2) whether the evidence is relevant to an issue at trial. *United States* v. *Guang*, 511 F.3d at 121. On the first question, the Harvard Evidence would be offered to show both Martoma's knowledge of the need to commit the offense in a way that avoids as much as possible detection through computer forensics and Martoma's demonstrated capacity to manufacture electronic forgeries to serve as defenses. On the second question, the issue of whether or what aspects of the Harvard Evidence are relevant to disputed issues depends predominantly on defenses the defendant may choose to offer.

The evidence relating to Martoma's forging of documents in connection with his expulsion would be introduced for a proper purpose because it is probative of "special capacity, ability or knowledge that would enable him to commit the crime," *United States* v. *Maravilla*, 907 F.2d at 222, and to do so in way that limited the risks of detection through electronic evidence. As an initial matter, the draft PowerPoint presentation that Dr. Gilman received on July 17, 2008 was an extraordinary piece of inside information, representing the secret results of a highly anticipated drug that were then known only to a small group of individuals. Any unauthorized person caught having possessed such a document prior to trading on its contents – particularly causing a nearly $1 billion sell-off in securities as Martoma is charged with doing – would be deeply incriminated by this finding.

Martoma, though, knew more than just that being caught in possession of the PowerPoint presentation would be powerful evidence of insider trading. Martoma, through his experience with the Ad Board, knew in the deeply personal way that life-altering personal experiences teach that electronic communications such as e-mails leave electronic footprints that are hard to alter or remove. Martoma would therefore have known the pronounced danger of obtaining the PowerPoint presentation through means most likely to leave traceable electronic footprints, such as receiving the document through his work e-mail before it was presented publicly.[5] Accordingly, Martoma would have been unlikely to have requested an electronic copy of the PowerPoint presentation through any means that could create such an obvious forensic record readily traceable to him. Moreover, no matter how Martoma obtained access to the document, he would have, upon recognizing the enormity of the profits and avoided losses obtained through

[5] At the time, SAC systematically deleted e-mails every 30 days unless the SAC employee took affirmative steps to retain the e-mail. Nonetheless, given the experience at Harvard with e-mail evidence and his ultimate expulsion, it is very unlikely that Martoma would have requested that such a sensitive document be e-mailed to him at work.

early access to the presentation, used his knowledge of computer forensics to do everything possible to destroy or alter any electronic evidence that could incriminate him. In fact, Martoma's demonstrated capacity to create elaborate electronic forgeries – which included expertise with respect to altering the dates of electronic records – could have been employed by Martoma to generate phony evidence purporting to show that Martoma had received the document only once it had become public. Indeed, were such evidence to be presented, it would be sufficiently consistent with the same approach Martoma had attempted in the Ad Board proceedings by altering an e-mail date to make it appear inculpatory as to be admissible to establish Martoma's modus operandi. *See United States v. Sliker*, 751 F.2d 477, 487 (2d Cir.1984) ("The similarity sufficient to admit evidence of past acts to establish a recurring modus operandi need not be complete; it is enough that the characteristics relied upon are sufficiently idiosyncratic to permit a fair inference of a pattern's existence.")

The next inquiry for the Court is whether the evidence relating to Martoma's knowledge and capacity with respect to forensic alteration is "relevant to a disputed issue in the case." *United States* v. *Guang*, 511 F.3d at 121. To the extent the defendant makes arguments that the Government's failure to recover electronic forensic evidence that Martoma had access to the PowerPoint presentation prior to the announcement casts doubt on whether Martoma in fact did have access to this document or the credibility of witness testimony to the contrary, the Harvard Evidence would be relevant as a counterpoint. It would establish that Martoma had knowledge of just how damaging such electronic evidence could be and support and argument that Martoma would have therefore taken pains to obtain access to the document in a way that left a limited forensic record and/or would have long ago destroyed or altered whatever forensic evidence did exist.

The Government's Harvard evidence becomes more relevant still in the event that the defense goes beyond arguing the absence of evidence to arguing that there is forensic evidence demonstrating that Martoma never had access to the PowerPoint presentation at any time before the public announcement. To the extent that there are legitimate questions as to the forensic reliability of such evidence and/or whether it was intentionally created for the purpose of protecting Martoma should his numerous consultations with Dr. Gilman come to light, it would be highly relevant to the jury's weighing of such evidence to know that Martoma had a demonstrated capacity to forge documents and create a phony forensic record (one that in this case might be difficult or impossible to disprove given that the events happened over five years ago). There may be other circumstances where the defendant makes arguments or offers evidence that make portions of the Harvard Evidence relevant – such as, for example, affirmatively putting Martoma's character or academic record into play in a way that is misleading without such evidence. As the full panoply of potential defense arguments that might open the door to the Harvard Evidence are unknown, the Government may identify additional issues implicating the Harvard Evidence as trial proceeds.

Finally, with respect to the Rule 403 analysis, there is no question that evidence that Martoma had forged evidence and altered forensic documents would not be viewed favorably, but it would not be *unfairly* prejudicial to introduce such evidence in the event that Martoma's defense involves arguments about electronic evidence that cannot be fairly weighted without evidence of Martoma's knowledge and capacity in this area. Indeed, the unfair prejudice would be to the Government if Martoma were, for example, to offer purportedly exculpatory electronic evidence of dubious province or validity without the jury's knowledge of Martoma's ability to manufacture such material. Additionally, the admissibility of the Harvard evidence would not of

course have to be an all-or-nothing determination, and certain facts relating to Martoma's forging of documents with lesser relevance to the particular defense that could cause unfair prejudice could be omitted, including, for example, through the redaction of documents offered into evidence. The Court could also give a limiting instruction to the jury explaining the proper purpose for the Harvard Evidence, which the Second Circuit has repeatedly held to be a sufficient remedy to cure residual prejudice. *See United States v. Pipola*, 83 F.3d 556, 566 (2d Cir. 1996); Rosa, 11 F.3d at 334. Finally, offering the Harvard Evidence or portions thereof need not lengthen the trial or otherwise distract from the core issues because the Harvard Evidence could be admitted largely through statements made and evidence conceded by Martoma in the Ad Board proceedings.

CONCLUSION

For the reasons set forth above, the Government respectfully requests that the Court permit the Government to offer such portions of the Harvard expulsion evidence under Rule 404(b) as are made relevant by the defense that is ultimately presented.

Dated: December 6, 2013
New York, New York

Respectfully submitted,

PREET BHARARA
United States Attorney

By: _____
Arlo Devlin-Brown
Eugene Ingoglia
Assistant United States Attorneys
Tel. No.: (212) 637-2506/2270

DISCIPLINARY HEARING ON CHARGES AGAINST AJAI MATHEW THOMAS

FINDINGS OF FACT AND DECISION OF THE ADMINISTRATIVE BOARD

The following facts are not in dispute, and the Board so finds:

1. In December 1998, Mathew Thomas altered the transcript of his first-year grades at Harvard Law School as follows: Civil Procedure, B to A; Contracts B+ to A; Criminal Law, B to A. Grades in Torts (B+), Property (A), and Negotiation (A-) were not changed. (Exh. 12)

Mr. Thomas has stated that he prepared the altered transcript with the intention that it be shown only to his parents.

2. At the end of December or in early January, Mr. Thomas's application for a clerkship was sent to 23 judges in the United States Courts of Appeals. The applications included the altered transcript.

Mr. Thomas has stated that it was his intention that the real transcript be sent with his applications. According to his statement, he arranged with his brother for the latter to prepare the packets of materials for mailing to each judge; his brother came across the altered transcript and, mistakenly believing that it was the real transcript, included it with the applications.

3. Not later than the weekend of January 23-24, Mr. Thomas was aware that the altered transcript had been sent to the judges. (Exh. 10, p. 4; Tr. Ap. 28, 240)

4. On January 26 and 27, Mr. Thomas interviewed for a clerkship with Judge Sentelle, Judge Randolph, and Judge Ginsburg of the United States Court of Appeals for the D.C. Circuit. Mr. Thomas did not disclose to the judges that the transcript that they had received was not accurate.

Mr. Thomas has stated that it was his intention, in order to avoid any harmful effect from the altered transcript, not to be offered a clerkship and that he tried not to be a successful candidate at the interviews. (Exh. 10, pp. 4-5; Tr. May 4, 131-133)

5. Two of the three judges who interviewed Mr. Thomas thought after the interviews that he was an extremely attractive candidate for a clerkship. One judge decided to offer him a clerkship.* He reported that Mr. Thomas's conduct at the interview was consistent only with his wanting the job. The second judge regarded Mr. Thomas as one of two finalists for a clerkship and chose the other person on the basis of an unusually strong recommendation. He reported

* The judge called Mr. Thomas late on the night of February 2, to offer him a clerkship. Because Mr. Thomas appeared to have been asleep and to have been awakened, the judge did not then offer him the job and asked him to call the next morning (February 3). When Mr. Thomas did not call, the judge's secretary or clerk called and left a message asking Mr. Thomas to call. Again the next day (February 4), a message was left for Mr. Thomas asking him to call. On the following day, February 5, the judge received a letter from Mr. Thomas dated January 31 and postmarked February 3, withdrawing his application. (See Finding 11 below.)

that Mr. Thomas "made a very good impression" and that he "almost hired" him. The third judge recalled nothing to suggest that Mr. Thomas was trying not to have a successful interview.

6. During the first week of January, Registrar Stephen Kane was informed by a clerk in the office of a judge to whom Mr. Thomas had applied that the transcript appeared not to be correct. Mr. Kane checked the grades and found that the transcript had been altered.

7. On February 1, shortly before 9:00 p.m., Mr. Thomas sent an e-mail message to Sandra Mays, secretary to Professor Horwitz, who had agreed to write a letter of recommendation for him. The message read: "just checking to make sure everything is in order for clerkship stuff. amt" (Exh. 6)

8. In the afternoon of February 2, Mr. Thomas came to Mr. Kane's office in response to a telephone message from Mr. Kane asking him to do so. Mr. Kane told Mr. Thomas that the altered transcript had been detected. Mr. Thomas acknowledged that he had altered the transcript. He told Mr. Kane that "it was all a joke" (Exh. 10, p. 6; Tr. Ap. 28, 40)

9. On February 2, after speaking with Mr. Kane, Mr. Thomas talked with Suzanne Richardson, Dean of Students. Mr. Thomas told her that "the application was a joke and that [he] really did not intend to pursue a clerkship." He told her also that he "had already sent withdrawal letters to the judges." (Exh. 10, pp. 6-7)

10. On the night of February 2, at about 10:20 p.m., an e-mail message from Mr. Thomas was transmitted to Sandra Mays. The message asked Ms. Mays not to send out letters of recommendation because "I am no longer looking for a clerkship." (Exh. 5, 3[1])

11. A letter withdrawing his application for a clerkship, dated January 31, was received by the judges to whom Mr. Thomas had applied. (Exh. 2) The letters were postmarked February 3. (Exh. 12)

12. Sometime after February 2 and before February 10, Mr. Kane learned that Mr. Thomas's letters to the judges withdrawing his application were postmarked February 3. Mr. Kane informed Dean Richardson, who informed Mr. Thomas before February 10.

13. In his written statement to the Administrative Board, dated February 17, Mr. Thomas stated that he had not already mailed the withdrawal letters when he met with Dean Richardson on February 2, as he had told her. He stated that he had already written the letters and had "stamped and addressed" them but did not mail them until the night of February 2. (Exh. 10, p. 7)

Two matters were the subject of extensive testimony at the hearings.

How the altered transcripts were sent.

According to the testimony of Mr. Thomas and his parents, he showed his parents the altered transcript, intended only for them, on December 24. (Tr. Ap. 28, 63, 74; Exh. 10, p. 3) According to his statement, several days later he "realized that what [he] had done was wrong and showed [his] parents [his] real grades." (Exh. 10, p.3) In the subsequent turmoil, he left the altered transcript on the desk in his room and "thought nothing more of it at the time." (Exh. 10, p. 3) Later, because he had to leave for an "impromptu" job interview in California (Exh. 10, pp. 3-4; Tr. Ap. 28, 234) he asked his brother to duplicate and assemble the materials for his applications for a clerkship. He left a copy of all the materials for the application—cover letter, writing sample, résumé, college recommendations—except the real transcript together in a packet in his room and put the transcript in a file cabinet, where he told his brother to find it. His brother, who knew nothing about the alteration of the transcript, saw the altered transcript on Mr. Thomas's desk, and, assuming it to be the real transcript, duplicated it and assembled it with the other materials. He then put the assembled applications in envelopes that Mr. Thomas had addressed. His mother mailed the applications, as she had agreed to do. She did not examine the materials before mailing them. (Exh. 10, pp. 3-4)

Most members of the Board have considerable problems with Mr. Thomas's account. They find it difficult to believe that, having, as he says, given time (a "couple of hours" – Tr. Ap. 28, 227) and attention to the alteration of the transcript in order to satisfy his parents' expectations and having observed their "ecstatic" reaction (Exh. 10, p.3), just a few days later he would have so completely changed his attitude that he revealed both that his grades were less good than they had appeared and that he had prepared a false transcript to deceive them. They find it difficult to believe that, having revealed his deception, he would have been so casual about the altered transcript and have left it visible on his desk where his brother would find it. They find it difficult to believe that, having the intention seriously to apply for a judicial clerkship and having prepared the materials for his application with care, he would have left the duplication and assembly of the materials for each judge entirely to his younger brother. They find it difficult to believe that he would have put all the materials for his application in plain view in one place and have put the real transcript alone inside his file cabinet (leaving the altered transcript separately in view). Mr. Thomas's father, mother, and brother testified that his account is accurate.

There are also some material inconsistencies in Mr. Thomas's account. He stated that he prepared mailing labels for the judges, to be sent with the application materials to Professor Horwitz, who had agreed to write letters of recommendation. (Tr. Ap. 28, 210, 233) But on January 28, Sandra Mays sent him an e-mail message that she needed labels for the judges. (Exh. 6) Mr. Thomas testified that when, in mid-January, he learned of his brother's mistake, he was "extremely angry" and they "had a huge argument." (Exh. 10, p. 4) His brother testified, however, that when Mr. Thomas learned of the mistake, he said something to the effect that "this was the wrong one" and the brother then "just left the room." (Tr. Ap. 28, 108, 114) There is some inconsistency in his brother's explanation of how he happened to see the altered transcript.

(Tr. Ap. 28, 114, 118-119) Although a lack of clarity is not surprising months after the event, the inconsistencies recounted here do not seem like details easily forgotten or misremembered.

Some members of the Board conclude without substantial doubt that Mr. Thomas's account of how the altered transcripts were sent is false and that he either sent the altered transcript or with knowledge or wilful ignorance caused it to be sent. Other members of the Board believe that although Mr. Thomas's account is highly improbable, there is insufficient basis to find with certainty that it is false. Accordingly the Board makes no finding on this issue. It adopts neither a mitigating finding that it was an accident that the altered transcript was sent to the Board nor a seriously aggravating finding that Mr. Thomas's account is false. In this respect, it relies only on Findings 3 and 4 above, that Mr. Thomas was aware that a false transcript had been sent to the judges and did not disclose that fact during his interviews.

The e-mail message to Sandra Mays, asking that Professor Horwitz's letters of recommendation not be sent. (Exh. 5)

It is conceded that this message was transmitted on February 2 at around 10:20 p.m. Mr. Thomas has stated that he composed the message on February 1 at around that time and, so far as he knew, sent it at that time. (Exh. 10, p. 6) The line at the top of the message indicates that it was sent on February 1 as does the message ID, which includes the date. (Exh. 5, line 4) The server log for the message (identified by the message ID), however, gives the date of transmission as February 2. (Exh. 3[1]) The date is significant because Mr. Thomas learned that the altered transcript had been detected in the afternoon of February 2. If he sent the message to Ms. Mays on February 1, that would indicate a change of heart before he knew that the alteration was discovered, as he asserts. (Exh. 10, p. 6) If, however, he sent the message on February 2, that would indicate not only that he had no change of heart until he knew that the alteration had been discovered, but also that he deliberately falsified the date of the e-mail message in an effort to fabricate evidence in his favor.

It is conceded that the message was actually transmitted on February 2. There is no plausible explanation for that date otherwise to appear on the server log. There is a further indication that the message was composed and sent on that date. The header of the message indicates that it was sent "In-Reply-To" a message that was sent on February 2 at about 9:19 a.m. (Exh. 5, line 3) That makes sense if the message was sent on February 2 at 10:20 p.m., but not if it was sent on February 1, since in that case it would have been sent about eleven hours before the message to which it was replying. (Exh. 6)

It is conceded that it is not difficult to change the date on a computer, which would then record the changed date on an e-mail message. There is no direct evidence that Mr. Thomas knew how to change the date on his computer on February 2; but he was accustomed to using a computer, and that operation is one with which many people are familiar. There is considerable evidence that Mr. Thomas was interested in that operation after February 2 (Tr. Ap. 28, 5, 23-24; May 6, 45, 67); but that might support an inference that he was not aware of it before that date or it might equally support an inference that he had changed the date and was concerned about whether the change could be detected.

Mr. Thomas explains the discrepancy between the date recorded on the top line and in the message ID of the e-mail message, on one hand, and the date on the server log, on the other, as follows: He wrote the message and tried to transmit it on February 1, but there was a disconnect between his computer and the system, which resulted in a failure of transmission. Although the computer would have signaled the failure, he failed to see the signal because immediately after (as he thought) transmitting the message, he started to work on another program, which obscured the e-mail screen. The message was then queued and was sent the next time he opened the Eudora e-mail program and was connected to the network, which was on February 2. No explanation has been offered for the "In-Reply-To" puzzle. Mr. Thomas testified that his computer was configured with a lot of shareware by his friends and that he did not know its full extent or what it did. Some such shareware, he suggested, might account for the puzzle. (Tr. May 4, 96-99, 102-105, 108) There was considerable reference during the hearings to Cybercreek, a program that, it was suggested, is one such possibility. (Tr. May 4, 101-105) Without any evidence to show that Cybercreek was installed on Mr. Thomas's computer and that its auto-responder had been configured to produce the result in question, the suggestion is wholly speculative.* Mr. Thomas's computer was sent by his counsel to several computer experts for analysis. (Tr. Ap. 28, 164, 172-173, 174, 184; May 4, 3) One expert who was expected to testify specifically about the "In-Reply-To" puzzle and whose credentials were presented to the Board (Exh. 15) did not testify because "he did not feel that he was in a position to authenticate . . . Matthew's [sic] version of the events." (Tr. May 4, 4) The computer itself was offered for examination during the hearings but in the end was not produced because counsel were unable to trace it and retrieve it in time. (Tr. May 4, 7-8, 91; May 6, 135) No concrete explanation for the puzzle was offered. All the persons who testified as computer experts agreed, however, that computers break down in strange ways, and none testified that, however unlikely it was, it was impossible for the occurrence to have happened as Mr. Thomas suggests.

Some members of the Board are convinced that Mr. Thomas altered the date on his computer and back-dated the e-mail message to Sandra Mays in an effort to deceive the Board. Other members believe that although it is more probable that Mr. Thomas altered the date than

---

* On May 12, after the hearings had been concluded and the Board had completed its deliberations, Mr. Thomas's counsel sent the chairman of the Board a letter stating the following:

> "Since I did not hear from you or the Committee, I returned the laptop to Mathew last evening. I was present when he opened the computer and turned it on for the first time to make sure that it was not damaged.
>
> "While checking the program directory, Mathew confirmed that he had the CyberCreek/CAR program installed on his computer. Subsequently, upon further examination, Mathew also confirmed that he had installed the RDM program described by Mr. Brunner in his letter dated May 11, 1999. I attach a printout from Mathew's directory describing the RDM application which is on Mathew's computer. As you can read, RDM on Mathew's computer is, in fact, shareware, and provides an autoresponder for the Eudora account. Although Mathew does not understand the technical operation and interaction of these programs, it is certain that the system was on his computer when he sent the e-mails in question on February 1, 1999."

It is difficult to know what to make of this information, since Mr. Thomas would presumably have been familiar with the program directory and the experts who were consulted by Mr. Thomas's counsel while the hearings were in progress would presumably have been looking for a program like Cybercreek and evidently did not find it. In any event, the Board has made no finding about this issue; the additional information does not affect its decision.

that it happened because of some unknown computer operation or failure, there is insufficient evidence so to conclude with certainty. The Board makes no finding on this issue. It adopts neither a mitigating finding that he sought to send the e-mail message on February 1 nor a seriously aggravating finding that he composed and sent the message on February 2 and back-dated it to February 1.

Although the Board has relied on uncontested facts, Mr. Thomas's manner before the Board did not lend credence to his account. Some members of the Board found him to be evasive and not forthcoming. The Board was impressed also by the cumulation of improbable occurrences in his account, which made it more difficult to accept his explanation of individual events.

Mr. Thomas has had an excellent record at the Law School academically and as a member of the community. He is a member of the Board of Student Advisers, an editor of the Journal of Law and Technology, and a co-founder of the Society of Law and Ethics. He was a semi-finalist in the Upper Round Ames Competition and received an award for the best brief in the first-year competition. He has been a research assistant for two professors, and was asked to be a teaching fellow for a professor. (Because of a schedule conflict, Mr. Thomas did not act as a teaching fellow. (Tr. Ap. 28, 30-31)) Two professors agreed to write letters of recommendation for him. A professor appeared as a witness for him at the hearing. Mr. Thomas also has an outstanding college record.

The Board notes that Mr. Thomas was apparently under extreme parental pressure to excel academically.

The Board's findings, stated above, are that Mr. Thomas falsified his transcript, interviewed with judges under false pretenses, and gave untruthful answers to questions of administrators at the Law School. These findings have led the Board to conclude that Mr. Thomas should be dismissed from the Law School. The Board believes that the falsification of a transcript in any circumstances is a serious matter. The transcript is a formal record, the integrity of which is essential to the legitimacy of the School and the certification of its graduates. The misrepresentation of an altered transcript to a public official is especially serious. Whether or not Mr. Thomas originally intended to deceive the judges to whom he applied for a clerkship, his failure to correct the mistake when, according to his testimony, he discovered it and his conduct of interviews with judges without revealing the truth were effectively an adoption of the misrepresentation as his own. The Law School's relationship with judges and their confidence in the honesty of its students is an asset of great importance to the school and to students individually, which Mr. Thomas's conduct undermined. The deception of administrators is inconsistent with membership in the Law School community and affects the community as a whole. In view of all of the above, and taking into account the factors stated above that might mitigate his wrongdoing, the Board believes that a sanction less than dismission is not appropriate.

The Board will recommend to the faculty that Mr. Thomas be dismissed. If the Board's recommendation is adopted by the faculty, the dismissal shall take effect as of this date. If the Board's recommendation is not adopted and a more severe sanction is not voted by the faculty, Mr. Thomas shall be suspended for five years, the suspension to take effect as of this date.

Administrative Board

May 12, 1999

Exhibit 4

Subject: clerkship recommendation
Date: Mon, 1 Feb 1999 22:23:33 -0500
From: amthomas@law.harvard.edu
To: btidd@law.harvard.edu

bethany,

please don't mail out recommendations on my behalf as I am no longer looking for a clerkship. thanks. please confirm that you have received this email.

mathew

(5)

amthomas@law.harvar, 10:20 PM 2/1/99 -, Re: Clerkships

Return-Path: <Thomas_Ajai_M@law.harvard.edu>
Date: Mon, 1 Feb 1999 22:20:56 -0500
In-Reply-To: <3.0.3.32.19990202091957.007c4990@pop.law.harvard.edu>
Message-Id: <3.0.2.16.19990201222056.4d7727be@pop.law.harvard.edu>
Subject: Re: Clerkships
MIME-Version: 1.0
Sender: amthomas@law.harvard.edu
To: mays@law.harvard.edu
From: amthomas@law.harvard.edu
Content-Type: text/plain; charset="us-ascii"
Content-Disposition: inline; filename="Re:"
Content-Transfer-Encoding: 7bit

sandra,

please don't mail out any recommendations on my behalf as I am no longer looking for a clerkship. thanks.

mathew

–Computer Data Forensics–
445 Park Avenue, 9th floor
New York, NY 10022

June 30, 1999

Administrative Board
Harvard Law School
Cambridge, MA 01238

VIA FACSIMILE
DICTATED BUT NOT READ

RE: Mr. Thomas
CDF Case File: thomasm19572

Our firm, Computer Data Forensics (hereinafter, "CDF") was retained by Mr. Thomas to conduct an investigation regarding Mr.Thomas' SONY Notebook (model# CPCG-505G, Serial# 289822 30311437, with port replicator model# PCGA-PR5, Serial# 28990800108 2841 and power source 16V AC Adapter serial# 9807A004679, Model PCG-AC51, all in bag marked Wet Suit 1.1 Patent Pending, Silicon Sport, color black). We received Mr. Thomas' laptop computer via Federal Express on May 26, 1999 at approximately 11:35 A.M. The laptop computer was moved to a secured location at which time, Case Analysts, Patrick Oxley, Robert Owens and Charles Clarke, removed the laptop computer from the Federal Express box. While the laptop computer was in CDF's possession, proper chain of custody was maintained at all times. Because we did not dismantle the computer, we did not take pictures of the laptop computer from various angles to document the system hardware components and how they were connected.

The laptop computer was not operated and computer evidence was not processed until bit stream backups were made of the hard disk drive utilizing SafeBack copies to preserve all data contained on the hard disk. It even circumvents attempts to hide data in bad clusters and bad sectors. All evidence processing was done on a restored copy of the bit stream backup rather than on the original computer. We proceeded to make a mirror image of the computer disk drive using the RSA algorithm. Although we typically use 32 bit algorithms, which are inherent in CRCHECK and CRC32, we were asked by the client to use elevated standards.

We used CRCMD5 to authenticate data at both a physical level and a logical level to demonstrate that we did not alter any of the evidence after the computer came into our possession. We proceeded with our investigation on two fronts: UNIX and PC. The UNIX Investigation is detailed in CDF Binder Number 1. The PC Investigation is detailed in CDF Binder Number 2. Both binders are in the possession of CDF. These binders merely contain work products. All pertinent findings have been delineated in this letter.

We have been asked to clearly delineate what software was utilized to perform our tests so that these tests may be reproduced. CDF utilizes the following software: GetFree, IPFilter, GetSlack, EnCase, FileList, FCG Analyzer, Partition Magic, and Anti-Clean. These software packages are utilized by law enforcement agencies and forensics experts throughout the country.

The Windows swap file is a valuable source of evidence and leads. With Windows 98, the swap file by default is set to be dynamically created as the computer is operated and when the computer is turned off, the swap file is erased. The content of the swap file captures and evaluates with GetFree. This software automatically captures erased file space and creates a file that can be evaluated by IPFilter.

The evaluation of the swap file was performed with IPFilter. This software relies upon artificial intelligence fuzzy logic to identify patterns of text associated with prior Internet activities. IPFilter

indicated that Mr. Thomas' laptop computer did indeed have the following URLs: www.cybercreek.com and www.consumerdeals.net and that they were accessed prior to February 1, 1999.

File slack is a data storage area of which most computer users are unaware. It consists of raw memory dumps that occur during the work session as files are closed. The data dumped from memory, ends up being stored at the end of allocated files, beyond the reach or the view of the computer user. GetSlack captures file slack and Encase was used to view and evaluate file slack. GetSlack indicated that the withdrawal letter showed a file creation date of January 31, 1999. GetSlack also indicated that the email sent by Mr. Thomas to Sandra Mays was created on February 1, 1999. Again, the file slack in the email is consistent with the email having been created on February 1, 1999. GetSlack also verified the creation date of the CyberCreek CAR Program on Mr. Thomas' laptop as January 6, 1999, the CAR/Eudora Interface as January 31, 1999, and a patch file program to correct an error in the CAR/Eudora Interface as February 4, 1999.

The DOS and Windows delete functions do not completely erase file names or file content. Many computer users are unaware that the storage space associated with such files merely becomes unallocated and available to be overwritten with new files. Unallocated space potentially contains erased files and file slack associated with the erased file. GetFree quickly captures all unallocated space from hard disk drives and floppy disks. GetFree indicated that the erased files and file slack associated with the erased files did not contain evidence pertinent to this situation.

From an evidence standpoint, file names, creation dates, last modified dates and times can be relevant. Therefore, it is important to catalog all allocated and erased files. FileList generates its output in the form of database file. The file can be sorted based on the file name, file size, file content, creation date, last modified date and time. Such sorted information comprise a time line (refer to Appendix 1) of computer usage. FileList indicated that from a timeline basis, Mr. Thomas' version of events is accurate.

Encrypted, compressed, and graphic files store data in binary format. As a result, text data stored in these file formats cannot be identified by a text search program. FCG Analyzer indicated that there were no encrypted, compressed, or graphic files pertinent to this situation. Manual evaluation of these files is required and in the case of encrypted files, much work may be involved. Reviewing the partitioning is important because the potential exists for hidden partitions and/or partitions formatted with other than a DOS compatible operating system. When this situation exists, it is comparable to finding a hidden hard disk drive and volumes of data and potential evidence Partition Magic indicated that there was neither hidden hard disk drive nor any potential evidence.

We then proceeded to use Anti-Clean, which was obtained by our contact at the International Association of Computer Investigation Specialists (IACIS) to determine if M-Sweep had been used on the laptop computer. M-Sweep is a software tool developed by New Technologies, Inc. (NTI) which eliminates all traces of ambient data in file slack and unallocated (erased file space). We determined that M-Sweep had not been used.

Our conclusion is that the computer data forensics evidence corroborates Mr. Thomas' assertion that he created the withdrawal letters on January 31, 1999 and sent the subject e-mail to Sandra Mays at her electronic mail address mays@law.harvard.edu at 10:20 PM the night of Monday, February 1, 1999. A variety of factors can delay the delivery of electronic mail messages, and we have reviewed computer data forensics evidence, which demonstrates the following series of events.

(1) Mr. Thomas' computer was connected to Harvard Law School's (HLS) modem pool from 9:40 PM until 9:54 PM the night of Monday, February 1, 1999, when the connection was terminated.

(2) Mr. Thomas' computer was connected to American Online (AOL) from 10:12 PM to 10:48 PM the same evening, February 1, 1999, to access MIT's computer systems (Please refer to AOL Invoice).

(3) Mr. Thomas' computer had a program running on his computer which ensured the clock in his computer was set accurately to facilitate his connection with MIT's computer systems (Please refer to Michael J. Sadaway Letter).

(4) Mr. Thomas used a friend's computer account to access MIT's computer system (Please refer Nathan Larson Letter).

(5) Nathan Larson's account accesses MIT's computer system using kerberized telnet, a UNIX communications process designed to ensure secure communications (Please refer to Eric Mumpower Letter).

(6) Manuel Wilson z-writes Mr. Thomas around 10:15 PM on February 1, 1999 to inquire how he was and how he was dealing with the important e-mail he needed to send (Please refer to Manuel Wilson Letter).

(7) Mr. Thomas sent an email to Sandra Mays (Mays) at 10:12 PM on February 1, 1999 through Eudora from his HLS account amthomas@law.harvard.edu

(8) Due to a conflict between AOL and Eudora configured for kerberization capacity, Mr. Thomas' email was not delivered to Sandra Mays on February 1, 1999, but was automatically queued in Eudora for delivery upon a successful connected. This prevented the e-mail messages he composed from being delivered until he reconnected to the HLS modem pool on February 2, 1999.

(9) While queued in Eudora, Mr. Thomas' email was routed through a shareware program CyberCreek CAR and its Car/Eudora Interface. CAR is a program that "creates, stores, forwards, replies to, and or deletes email messages from a POP3 email account." The program scans the "TO:" and "FROM:" headers of any queued message and compares them to an incoming message's headers. If the incoming message's headers match a queued message, the program sends the queued message as a "IN REPLY TO" response to the incoming message. (Please refer to CyberCreek Letter and description of CAR/Eudora Interface).

(10) When Mr. Thomas logged onto Eudora on February 2, 1999 through the HLS modem pool, an incoming message from Sandra Mays was received by Eudora. The CAR program detected the incoming message from Sandra Mays, and, since the message headers of Ms. Mays incoming message matched Mr. Thomas' queued message, the CAR program sent Mr. Thomas' email as an "IN REPLY TO" response to Ms. Mays' email. This occurred even though Mr. Thomas' email was created and queued in Eudora one day prior to the receipt of Ms. Mays' email.

We have also been asked to examine three additional emails peripherally related to this matter. These emails appear to be sent earlier than the date recorded in Mr. Thomas' HLS email logs. GetSlack indicates that the creation dates for these three emails are accurate. Further analysis suggests that time delays may be accounted for by errors in the CAR/Eudora Interface. At least one technical opinion of the program suggests some problems with the interface package that might result in sent messages being unintentionally queued and resent at a later time through Eudora. This problem can be corrected by a shareware patch file available on the Internet. Our test suggests that Mr. Thomas installed this patch on February 4, 1999, and the logs reflect no further email inconsistencies except for one test email message sent by an HLS technician examining Mr. Thomas' computer on February 14,1999, who claims responsibility for the modifications. (Please refer to Daniel Kassabian Letter).

This concludes our analysis of Mr. Thomas' laptop. If you have any questions about our analysis or require additional information, please do not hesitate to contact Charles V. Clarke directly at 917-322-2171 or at the Computer Data Forensics main telephone number 212-560-5159.

Signed under the pains and penalties of perjury this 30th day of June 1999.

Sincerely,
Case Analyst Team TR

Charles V. Clarke
Case Analyst & Project Manager
CDF ID# 919273
SS# [redacted]

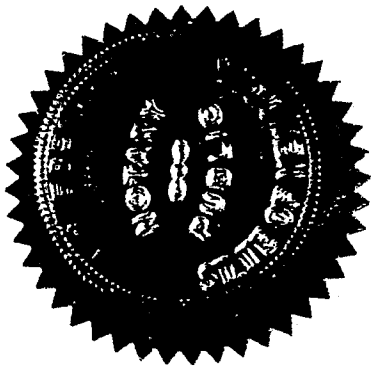
Patrick A. Oxley
Case Analyst & Engineer
CDF ID# 9192721
SS# [redacted]

Robert C. Owens
Case Analyst & Quality Assurance/
Quality Control Representative
CDF ID# 919272
SS# [redacted]

Enclosures: (1)
Rcd: file

cc: Mathew Thomas

LUIS ESPINOSA
Notary Public, State of New York
No. 31-4927002
Qualified in New York County
Commission Expires [illegible]



Computer Data Forensics

SERVICES
PRICING AND POLICY
SET UP AN ACCOUNT
USE OUR SERVICE
FAQ

SERVICES

Computer Data Forensics offers a vast array of services to collect, preserves, analyze, and present computer-related evidence. CDF's computer forensics analysis can be useful in a variety of settings, such as criminal or civil, and can help authenticate the validity of data to establish when it was created, accessed, or destroyed. Through CDF's online global registry, computer data can be easily submitted, and the precise time, date and contents of any digital file can be certified and validated. Together, CDF's forensics expertise and proprietary registration technology provides one of the most thorough verifications of computer data available today.

Computer Data Forensics draws on an array of methods for discovering data that resides in a computer system or recovering deleted, encrypted, or damaged file information. Using the latest techniques and software in computer forensics investigation and recovery, CDF can establish whether important records have been hidden, altered, or tampered with after a given date. CDF';s elevated standards of analysis enable it to discover and potentially to recover all files on the subject system. These includes existing normal files, uncover hidden files as well as temporary or swap files used by both the application programs and the operating system.

Computer Data Forensics can also verify or reconstruct patterns for computer activity at the hardware and software level. These patterns might explain why events such as a computer failure occurred and what effects a computer failure might produce both internally and in networked systems.

Computer Data Forensics provides a report of its overall analysis of the subject computer system, as well as a listing of all possibly relevant files and discovered file data. Further, CDF provides an opinion of the system layout, the file structures discovered, ay discovered data and authorship information, any attempts to hide, delete, protect, encrypt information, and anything else that has been discovered and appears to be relevant to the overall computer system examination.

Electronic Storage

CDF's on-line registry allows clients the ease of submitting their files through the Internet. CDF will store this information and maintain a proper "chain of custody" to ensure that your information is not tampered with or altered by others. Our system permits users easy, 24-hour access to their files while in our possession. Stored records are subject to forensic analysis below.

Forensic Analysis

CDF will search through your files for any relevant evidence. The work will be performed in our labs by trained experts to ensure a

through, careful forensic analysis.

During the forensic analysis, our experts use a variety of techniques to discover hidden or deleted evidence. In doing so we are able to recreate an event or chain of events to explain various computer scenarios or to verify your version of electronic events. Sometimes these efforts lead to a fairly detailed picture of fraud, sabotage, or conspiracy. Even bits of data we are able to show inappropriate behavior.

Computer Data Forensics

PRICING AND POLICIES

CDF'S PRICING

CDF's fee structure varies according to the level of analysis required and teh testing standards requested by our clients. Please inquire about our affordable pricing structure.

CDF'S POLICY

When setting up an account, CDF asks you to select a private password that will allow you to enter the CDF registry, track your registration history, verify new files or retrieve information on previously examined files. The password is encrypted for your protection so CDF never sees it. Please select something easy to remember and keep a record of it for future reference because if you lose your password, you will have to contact CDF for a replacement.

PRIVACY POLICY

CDF adheres to strict privacy policies with regard to your data files. The contents of this information will not be revealed unless required by a valid court order.

Computer Data Forensics

SIGNUP LOGIN

HOME ABOUT US SIGNUP LOGIN TRACKING HELP/SUPPORT CONTACT US

- SERVICES
- PRICING AND POLICY
- SET UP AN ACCOUNT
- USE OUR SERVICE
- FAQ

Contact Information

Computer Data Forensics
300 Park Avenue, 17th Floor
NY, NY 10002

Tel: 212.560.5159
Fax: 212.714.1353

Computer Data Forensics

SIGNUP LOGIN

HOME ABOUT US SIGN UP LOGIN TRACKING HELP/SUPPORT CONTACT US

- SERVICES
- PRICING AND POLICY
- SET UP AN ACCOUNT
- USE OUR SERVICE
- F A Q

ABOUT COMPUTER DATA FORENSICS:

Computer Data Forensics provides clients with an analysis of a number of operating systems and their associated storage media. Our elevated standards of security ensure that these examinations produce results that are valid and can be admitted in criminal, civil, or other proceedings

CDF has the ability, experience, and desire to assist in technical investigations. CDF will provide quick, competent, complete examinations of your computer that will address your issues. CDF will present you with the evidence or data in an understandable format for your audience. Our reports will describe our procedures and protocols, show what evidence or data was recovered during the examination and discuss the significance of any technical issues or opinions in an easily understandable manner.

We provide expert forensic computer investigative assistance to a number of groups including:

Businesses
Government agencies
Corporations
Law firms
Accounting firms
Law enforcement
Prosecutors Defense Counsel
Administrative Agencies

WHY CHOOSE COMPUTER DATA FORENSICS?

First, CDF will help you uncover inaccessible date. Using proprietary computer evidence tools and techniques, our experts can recover and analyze data that cannot be accessed through conventional means.

Second, CDF uses more sophisticated techniques than our competitors.

Third, CDF is cost-effective. Our resources and techniques are designed to be fast and efficient, thereby saving our clients in the long run.

Fourth, CDf can help you find the evidence that you need to make your case.

Computer Data Forensics' offers a broad range of expertise. CDF covers virtually every operating system and media type, including:

Operating Systems:
DOS
OS/2
Windows 95
UNIX/XENIX
Windows 3.x

Macintosh
Sun AS/400
NetWare R/6000

Drives:
Hard drives
Optical drives
Zip
Floppy diskettes

Computer Data Forensics

SIGNUP LOGIN

HOME ABOUT US SIGNUP LOGIN TRACKING HELP/SUPPORT CONTACT US

SERVICES
PRICING AND POLICY
SET UP AN ACCOUNT
USE OUR SERVICE
FAQ

FREQUENTLY ASKED QUESTIONS?

What are computers forensics examinations and why are they important?

Forensics examinations consist of a series of refined procedures and universal protocols to uncover missing data, hidden data, or deleted date. Exploring portions of commuters inaccessible to untrained personnel, these examinations go far beyond typical data recover. CDF's examinations are conducted at elevated standards to ensure that all data found is an accurate representation of the data that was on the original media and that the data found can be admitted in court, if necessary. In short, CDF's examinations are thorough, secure, and fully documented examinations of computers and associates storage media.

Computers evidence can be very important in any type investigation or inquiry. CDF uses a combination of hardware and software tools, as well as procedures to protect the original computer data, to recover hidden, erased, and password-protected data. All recovery and analysis work is performed on an exact copy of the original material. This practice ensures that the original materials are not accidentally altered or damages in some way.

Since there is a wide variety of computers, peripherals, and software available, including many different forms of storage (jazz, zip, CD-ROM, disk, etc.) your expert must possess the numerous skills and resources available for recovery and analysis of recovered data.

Why should we choose you to examine our computers?

CDF has considerable experience in the recovery and analysis of computer data examination. CDF's on-line registry allows for simple, accessible service. Together, CDF's forensics expertise and proprietary registration technology provides one of the most thorough verifications of computer data available today.

Who Uses CDF?

Businesses
Government agencies
Corporations
Law firms
Accounting firms
Law enforcement
Prosecutors
Defense Counsel
Administrative Agencies

Can I submit any type of computer date for forensic

analysis?

CDF's forensic analysis can be applied to files of the type specified. (SEE OPERATING SYSTEMS AND DRIVES).

How safe and secure is my submitted information?

CDF uses the highest level of security available. CDF also adheres to strict privacy policies. Files are routinely backed up as an extra layer or protection. Moreover, the file itself cannot be altered or viewed by anyone at the server site, and it is impossible for computer data to be altered, or backdated since it is only an image of the original materials, which are still in your possession.

We have computer personnel in our company, why shouldn't we let them conduct the examination?

There are several reasons to avoid company employees for sensitive computer forensic analysis. If the issue is important enough to see computer forensics analysis, then the integrity of your findings is of paramount importance. Using company employee can open you up to allegations of fabricating evidence and other impropriety. CDF provides independent analysis based on a foundation of integrity.

Likewise, company employees may be knowledgeable about certain areas of computers; however, they are unlikely to be trained in the refined protocols of forensic analysis. CDF protocols ensure that all available evidence is discovered and admissible for court if necessary. CDF also takes steps to safeguard computer data; these steps require specialized training in various hardware and software. CDF experts have the training, experience, and tools to conduct a thorough examination of computer data and the ability to interpret what they find.

How frequently should I have CDF analyze my files?

You can register at your convenience 24 hours/day. Only you can determine what is important enough to document and forensically verify. If you continually deal with sensitive information, you might consider registering important documents as part of a routine. If you are a one time user, CDF's thorough forensic analysis will still provide you with a detailed assessment of your files and can help verify your version of electronic events.

What is CDF's Online Registry?

CDF's registry is a global, online database that permits users to submit their documents for forensic validation of the precise time, date and contents of computer data. Registration is quick, easy, and efficient. Our tracking services enable clients to monitor their documents 24 hours a day from the convenience of their computer.

Can I submit files to CDF's registry from any computer?

Yes, CDF can be used from any computer with access to he Internet. You must use a compatible browser (currently AOL browser, Netscape Navigator or Microsoft Internet Explorer, Versions 4.0 or better).

What does it cost?

CDF's fee structure varies according the level of analysis required and the testing standards requested by our clients. Please inquire about our affordable pricing structure.

Computer Data Forensics

SIGNUP LOGIN

HOME ABOUT US SIGNUP LOGIN HACKING HELP/SUPPORT CONTACT US

- SERVICES
- PRICING AND POLICY
- SET UP AN ACCOUNT
- USE OUR SERVICE
- FAQ

VALIDATE YOUR RECORDS WITH CERTAINTY...SUBSTANTIATE YOUR VERSION OF ELECTRONIC EVENTS

Computer Data Forensics offers a vast array of services to collect, preserve, analyze and present computer related evidence. CDF's computer forensics analysis can be useful in a variety of settings, such as criminal or civil, and can help authenticate the validity of data to establish when it was created, accessed, or destroyed.

CDF has considerable experience in the recovery of computer data. Let our experience assist you. If it is important enough to consider computer forensic help, it is important enough to choose the best.